(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－355558

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.[6]	識別記号	ＦＩ
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387
5/92		5/92

審査請求　未請求　請求項の数１　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－122464

(22)出願日　平成11年(1999)４月28日

(31)優先権主張番号　０９／０７０－４７０

(32)優先日　1998年４月30日

(33)優先権主張国　米国（ＵＳ）

特許法第64条第２項ただし書の規定により図面第８図，第11図は不掲載とした。

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
ＨＥＷＬＥＴＴ－ＰＡＣＫＡＲＤ　ＣＯＭＰＡＮＹ
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000

(72)発明者　ピング・ワー・ウォング
アメリカ合衆国　カリフォルニア，サニーヴェイル，ノウルトン・ドライブ　1443

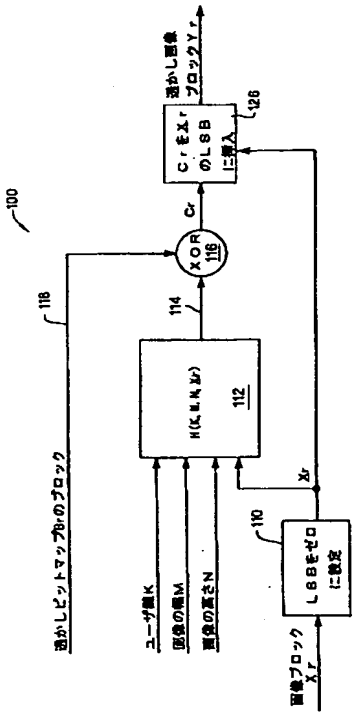
(74)代理人　弁理士　萩野　平　（外４名）

(54)【発明の名称】　透かし挿入装置

(57)【要約】

【課題】　ピクセル値のみならず画像サイズの変更も検出可能な、公開鍵あるいは秘密鍵透かし処理に使用できるデジタル画像の透かし挿入装置を提供すること。

【解決手段】　画像ブロックX_rの少なくとも一つの所定ビットを修正して、修正済み画像ブロック$\underline{X}_z$を生成する修正手段１１０と、暗号ハッシュ関数により値の摘要を計算しハッシュ出力１１４を出力する計算手段１１２と、ハッシュ出力１１４を透かし１１８と組み合わせ、合成画像ブロックC_rを生成する組み合わせ手段１１６と、修正済み画像ブロック$\underline{X}_r$の中に合成画像ブロックC_rを挿入し、透かし処理済み画像ブロックY_rを出力する挿入手段１２６とから構成される。



1

【特許請求の範囲】

【請求項１】　デジタル画像中に透かしを挿入する透かし挿入装置において、

画像ブロックX_r中の少なくとも１つの所定ビットを所定値に修正する手段であって、修正済み画像ブロックが$\underline{X}_r$である修正手段と、

暗号ハッシュ関数を使用して値の摘要を計算する手段であって、該手段の出力がハッシュ出力であり、前記修正手段に電気的に結合された計算手段と、

前記ハッシュ出力を透かしと組み合わせる手段であって、該手段の出力が合成画像ブロックであり、前記計算手段に電気的に結合された組み合わせ手段と、

前記修正済み画像ブロック$\underline{X}_r$に第１画像ブロックを挿入する手段であって、前記修正手段に電気的に結合された挿入手段と、を備えたことを特徴とする透かし挿入装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、所有権の検証および／または認証の目的で画像中に透かしであるデジタル識別子を挿入し、また、受け取った画像中のデジタル識別子を抽出する技術に関する。

【０００２】

【従来の技術】デジタル透かしは、所有権の検証および／または認証の目的でデジタル識別子を抽出することができるように、画像中にデジタル識別子を挿入する技術である。所有権の検証とは、所有者に関連していると識別することができる透かし処理された画像から、デジタル識別子を抽出することができることを意味する。認証とは、透かし処理された画像に対するどのような変更も検出することができることを指す。デジタル透かしは、ワールドワイドウェブ（WWW）および電子商取引でのデジタル画像の使用の普及のため、ますます重要になっている。

【０００３】画像を見る者の視点から、透かしは２つの範疇、すなわち可視および不可視に分類することができる。可視透かし処理は、可視スタンプ、例えば会社ロゴが画像中に挿入される透かし処理手順のクラスをいう。このスタンプは、現在の米国ドル紙幣の透かしと同様に可視である。Braudaway氏他の「Color Correct Digital Watermarking of Images」という名称の米国特許第５，５３０，７５９号公報に、元のデジタル画像中に可視の透かしを挿入する方法の記載がある。Braudaway氏他は、透かしの位置に基づいて元画像の明るさ、または暗さを修正することを教示している。該公報に記載されている透かし挿入方法および透かし抽出方法にはランダムノイズ成分が含まれるため、許可されたユーザを除いては、元画像から透かしを除去する困難さが増す。

【０００４】不可視の透かしは、その結果生じる画像が元の透かし処理をしていない画像と視覚的に区別できないように、デジタル画像に加えられるデジタル識別子である。不可視の署名を、デジタル画像上の一連の画像処理操作により抽出または検出することができる。I. J. Cox氏、J. Kilian氏、T. Leighton氏およびT. Shamoon氏の論文「Secure Spread Spectrum Watermarking for Multimedia」（Tech. Rep. 95-10, NEC Research Institute, １９９５年）は、デジタル画像中に不可視の透かしを挿入する方法を開示している。該論文は、画像の周波数領域表現への元画像の変換について記述している。該論文に記述された方法は、画像の周波数変換した表現から、視覚的に重要であるＮ個の画像の周波数成分を選び、この元画像の周波数成分に透かし処理信号を透かしとして挿入する。

【０００５】所有権の検証を実施する一方法は、透かし処理された画像から適切なユーザ鍵によってのみ所望の透かしを抽出できるように、ユーザ鍵を透かしと関連付けることである。２つの従来の透かし処理方法には、（１）所有者および受信者の両者が同じ秘密鍵を所有する必要がある秘密鍵透かし処理、および（２）２つの異なる鍵、すなわち、個人鍵およびそれに対応する公開鍵（共通鍵）を使用する必要がある公開鍵透かし処理が含まれる。個人鍵は所有者だけが知っている。公開鍵は秘密である必要はなく、透かしを検出するために画像の受信者によって使用される。秘密鍵の透かしについての問題は、実際の伝送の前に、通常は、よりコストのかかる秘密の代替パスを介して鍵の交換を行わなければならないこと、または送信者と受信者とが近接しているときに取り決めなければならないことである。

【０００６】M. M. Yeung氏およびF. Mintzer氏の論文「An invisible watermarking technique for image verification」（Proceedings of ICIP（米国、カリフォルニア州、サンタバーバラ）１９９７年１０月）は、秘密鍵システムに関する認証透かし処理方法を開示している。該論文が教示する方法では、秘密鍵が乱数発生器と共に使用され、ルックアップテーブルを生成する。ルックアップテーブルは透かし抽出手順を規定し、同様に、いくつかの調整を経た元画像への透かし挿入ステップを提案する。透かし抽出ステップにおいて、抽出した透かしは、元画像が修正されたかどうか判定するために既知の透かしと比較される。該論文による技術は、透かし処理された画像のピクセル値に対する変更を検出できるが、クロッピング（cropping）アルゴリズムまたはある種のスケーリングアルゴリズムから生じる画像サイズの変更は検出しない。

【０００７】

【発明が解決しようとする課題】所有権の検証と認証との両方の目的に使用することができ、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用される不可視の透かし処理技術が求められている。

【０００８】本発明は、上記事情に鑑みてなされたもので、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用でき、検証と認証との両方の目的に使用可能なデジタル画像中へ透かしを挿入する透かし挿入装置を提供することを目的とする。

【０００９】

【課題を解決する手段】本発明は、所有権の検証と認証との両方の目的に使用でき、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用される不可視のデジタル透かし処理技術を提供する。本発明は、画像所有者が使用する透かし挿入手順およびこれに対応する画像の受信者が使用する抽出手順を含む。透かし挿入手順は、修正済み画像ブロック、鍵および種々の画像パラメータのハッシュ関数を計算し、次いでハッシュ出力を１ブロックの透かしビットマップと組合せ、合成画像ブロックを生成する。好ましい実施形態では、修正済み画像ブロックは、そのＬＳＢをゼロに設定した元の画像ブロックである。透かし処理された画像ブロックを生成する最後のステップとして、合成画像ブロックが修正済み画像のＬＳＢ中に挿入される。

【００１０】透かし抽出手順では、透かし処理された画像ブロックを用いて、２つの異なる画像ブロック、すなわち透かし処理された画像ブロックのＬＳＢをゼロに設定した第１画像ブロックと、透かし処理された画像ブロックのＬＳＢを抽出した第２画像ブロックとを生成する。第１画像ブロック、鍵および種々の画像パラメータは、ハッシュ関数の入力として使用される。透かし抽出工程のためのハッシュ関数への入力は、透かし挿入工程のためのハッシュ関数への入力とは異なっているが、透かし挿入と抽出との両方に使用される暗号ハッシュ関数は同一でなければならない。ハッシュ関数が異なる場合、この透かしを適切に抽出することができず、抽出した透かし画像がノイズとして現れる。

【００１１】透かし抽出手順は、ハッシュ関数を使用して値の摘要を計算し、ハッシュ出力を生じる。ハッシュ出力は、好ましくは排他的論理和を使用して、第２画像ブロックと組み合わされる。第２画像ブロックを有する組み合わされたハッシュ出力の結果は、抽出された透かしの１ブロックである。

【００１２】上述の挿入および抽出方法は、同じ秘密鍵が透かし挿入と抽出との両方に使用される秘密鍵暗号化のために使用される。代替の実施形態では、前記方法が、画像の完全性および所有権を公開鍵を使用して検証することができるように修正される。この代替の実施形態において、透かし挿入手順では、公開鍵暗号化ステップが、ハッシュした関数を透かしビットマップと組み合わせるステップの後に入れられる。さらに、透かし抽出手順では、可逆排他的論理和論理関数を使用して、公開鍵解読ステップが透かしを抽出する前に入れられる。このようなシステムでは、画像の所有者は個人鍵Ｋ′を用いて透かしを挿入する。透かし抽出手順では、いずれの個人も、バイナリ（binary）透かしを抽出するために、（個人鍵Ｋ′に対応する）公開鍵Ｋを使用することができ、これによって透かし処理された画像に対して行われたあらゆる変更が示される。

【００１３】本発明は、秘密鍵と公開鍵との両方の透かし処理システムで透かし処理された画像に対するあらゆる変更を検出する認証技術を提供する。変更の検出は、例えば、画像が法律上の証拠として使用される場合、および画像の電子商取引において、この画像が売り手から買い手に配送される場合に、画像に対する変更がないことを画像の買い手に保証することができる。この画像のいずれかの部分が変更された場合、本発明による透かし抽出手順は変更された画像の特定の部分を示す出力を返す。透かし処理された画像が切り取られた場合、この抽出手順はランダムノイズに似た出力を返し、切り取られた画像が有効でないことを表す。

【００１４】本発明の性質および利点は、本明細書の以後の発明の実施の形態および図面を参照すればさらに理解できよう。

【００１５】

【発明の実施の形態】本発明は、Ｍ×Ｎピクセルの画像$X_{m,n}$の中にデジタル識別子を埋め込み、抽出して、同じサイズの透かし処理された画像$Y_{m,n}$を形成する技術を提供する。図１および図２に、本発明の第１の実施形態に基づく透かし挿入装置および透かし挿入方法を示す。図４および図５に、本発明の第１の実施形態に基づく透かし抽出装置および透かし抽出方法を示す。図４および図５に示す透かし抽出装置および透かし抽出方法は、図１および図２に示した透かし挿入装置および透かし挿入方法一緒に使用すべきである。

【００１６】図１のブロック図を参照すると、透かし挿入装置を実施するためのブロック図が示される。図２には、図１に示す透かし挿入装置に対応する方法のステップを示すフローチャートが示されている。図１を参照すると、本発明に基づいて、元の入力デジタル画像中への透かし挿入を実施するための透かし挿入装置１００は、画像ブロックX_r中の少なくとも１つの所定ビットを修正して、修正済み画像ブロック$\underline{X}_r$を生成する修正手段１００と、修正手段１１０が電気的に結合され、暗号ハッシュ関数を使用して値の摘要（digest）を計算し、ハッシュ出力１１４を出力する計算手段１１２と、計算手段１１２に電気的に結合され、ハッシュ出力１１４を透かし１１８と組み合わせ、該組み合わせによる出力が合成画像ブロックである組み合わせ手段１１６と、修正手段１１０に電気的に結合された、修正済み画像ブロック$\underline{X}_r$の中に合成画像ブロック（C_r）を挿入する挿入手段１２６とを含む。

【００１７】図２のフローチャートを参照すると、好ましい実施形態では、元の入力デジタル画像の中に透かしを挿入するための方法は、少なくとも１つのＩ×Ｊのブロック中に画像ブロックX_rを区分するステップ（１５０）と、各Ｉ×Ｊブロックごとに、該ブロックの少なくとも１つの所定ビットを所定値に修正するステップであって、前記修正済み画像ブロックが$\underline{X}_r$であるステップ（１５２）と、暗号ハッシュ関数を使用して値の摘要を計算するステップ（１５４）と、前のステップで計算したハッシュ出力を透かしビットマップB_rと組み合わせるステップであって、その場合、ハッシュ出力を透かしB_rと組み合わせるステップの出力は、合成画像ブロックC_rであるステップ（１５６）と、修正済み画像$\underline{X}_r$中に値C_rを挿入するステップ（１５８）とを含む。

【００１８】図２に示すステップは、図１に示す実施ブロック図に対応する。例えば、値の摘要を計算するステップ（ステップ１５４）は、図１の実施ブロック１１２に対応する。言い換えると、値の摘要を計算するステップは、ブロック１１２によって実行される。同様に、ステップ１５２はブロック１１０に対応し、ステップ１５６はブロック１１６に対応し、ステップ１５８はブロック１２６に対応する。図２に、図１のステップのフローチャートを示すが、図１に示すブロック図は、各ステップおよび一連のステップから生じる入力および出力を明示する。

【００１９】所定ビットを所定値に設定する手段への入力は、１ブロックの元の入力画像$X_{m,n}$である。好ましい実施形態では、元の入力画像$X_{m,n}$はサイズＭ×Ｎのグレースケール画像である。代替の実施形態では、元の入力画像はカラー画像である。カラー画像の場合、図１、図２、図３、図４、図５、図１２、図１３、図１４および図１５に示す同じ技術を、ＲＧＢカラー空間または、例えばＹＵＶ等の他の任意のカラー空間のどちらかにある画像のカラー平面に独立して適用することができる。

【００２０】好ましい実施形態では、画像$X_{m,n}$は、Ｉ×Ｊのピクセルのブロック中に区分される。一実施形態では、他のブロックサイズも可能であるが、本願記載の区分されたブロックは、８×８である。さらに、元の画像をＩ×Ｊのピクセルブロックに区分するステップが不要になる（これは、画像を１つのブロック中に区分することに等しく、画像ブロックはＩ＝ＭおよびＪ＝Ｎのブロックサイズを有する）。しかし、全体の画像に対してブロックを１つとするのは好ましくない。元の入力画像の区分は、画像を認証する時にローカライゼーション（localization）を維持する助けとなる。さらに、区分は、この画像を見る者が、画像の変更が生じた位置をより明確に見る助けになる。

【００２１】$X_{m,n}$中に埋め込むべき透かしを表す２レベル画像を$a_{m,n}$とする。$a_{m,n}$は、$X_{m,n}$と同じサイズ

である必要はないことに留意されたい。$a_{m,n}$から、（$X_{m,n}$と同じサイズの）サイズＭ×Ｎの別の２レベル画像$b_{m,n}$を形成することができる。画像$a_{m,n}$を、$X_{m,n}$と同じサイズの画像に変換する多くの方法がある。例えば、$b_{m,n}$は、$a_{m,n}$をタイル化（tiling）すること、すなわち定期的に$a_{m,n}$を所望のサイズに置き換えることによって形成されてもよい。別の可能性は、所望のサイズの$b_{m,n}$が得られるように、$a_{m,n}$の境界に全てゼロ（または、全て１）を添付することである。

【００２２】Ｉ×Ｊのピクセルブロックの中に区分された元の入力画像$X_{m,n}$について、

$X_r = x_{iI+k\,jJ+l}$（但し、$0 \leqq k \leqq I-1$、$0 \leqq l \leqq J-1$）

を画像$X_{m,n}$から得られる１ブロックのサイズＩ×Ｊであるとする。話を簡単にするために、単一インデックスｒを使用して、この画像中のｒ番目のブロックを示している。透かしビットマップ１１８に対するバイナリ画像$b_{m,n}$内の対応するブロックが、下式で表される。

$B_r = b_{iI+k\,jJ+l}$（但し、$0 \leqq k \leqq I-1$、$0 \leqq l \leqq J-1$）

ＩおよびＪは、$IJ \leqq p$を満足するならば、任意の数にすることができることに留意されたい。但し、ｐはハッシュ関数１１２のサイズである。

【００２３】画像ブロックの少なくとも１つの所定ビットを所定値に修正する修正手段１１０への入力が、画像$X_{m,n}$のｒ番目のブロックである。好ましい実施形態では、設定中のビットは、そのブロックのＬＳＢである。このブロックのＬＳＢを修正すると、最小の可視画像ゆがみが生じるが、これは不可視の透かしのための重要な要因である。図１に示す実施形態が好ましいが、画像ブロックX_rを修正するための代替の方法を使用することもできる。しかし、代替の方法を実施する場合でさえ、透かし挿入工程中の画像ブロックX_rを修正する（手段１１０、ステップ１５２ａ）ものと同じ方法を、図４および図５に示す透かし抽出工程の透かし処理された画像ブロックY_rを修正する（手段２１０、ステップ２５２ａ）ものにも使用しなければならないことは重要である。

【００２４】図１に示す実施形態では、画像ブロックX_rは、画像ブロックのＬＳＢをゼロに設定することによって修正される。ステップ１５２で実施された実施形態の代替の実施形態では、ＬＳＢ以外のビット（あるいは、１群のビット）は、所定値に設定される。図１に示す実施形態では、システム設計者によって決定された値を変更することができるが、この所定値はゼロである。前述のように、所定値および所定ビットの位置が、システム設計者によって変更できるが、図１で規定された透かし挿入手順に使用されたものと同じ所定ビットおよび所定値を、図４および図５で規定された透かし抽出手順にも使用しなければならないことは重要である。言い換

えれば、元の入力画像のブロックの所定ビットを所定値に設定する修正手段１１０が、所定ビットとしてその画像のＬＳＢを、かつその所定値として値ゼロを使用する場合、図４の所定ビットを設定する手段２１０は、所定ビットとしてその画像のＬＳＢを、またその所定値として値ゼロを使用しなければならない。

【００２５】図３に、画像ブロックX_rを修正するための様々な代替形態を示す。（図１に示す）第１の実施形態では、各ブロックごとに、画像ブロックX_rの所定ビットが所定値に設定される。しかし、代替の実施形態では、各ブロックごとに所定ビットが放棄される（ステップ１５２ｂ）。所定ビットが放棄される場合、合成画像ブロックC_rが、好適にはこの所定ビットに挿入される。第３の代替の実施形態では、画像ブロックは１パターンのビットに基づいて修正することができる（ステップ１５２ｃ）。所定のブロックがあるパターンに基づいて修正される場合、合成画像ブロックC_rが、好適にはこのパターンのビットに挿入される（ステップ１５８）。図３には、画像ブロックX_rを修正するための３つだけの可能な代替形態を示す。画像ブロックX_rを修正するために、他の代替形態も可能である。重要なことは、画像ブロックX_rが修正されることである。合成画像の少なくとも一部が、修正済み画像ブロック$\underline{X}_r$の修正されたビットに挿入されることが好ましい。

【００２６】画像ブロックのブロックの所定ビットを修正する手段の出力は$\underline{X}_r$である。$\underline{X}_r$は、暗号ハッシュ関数を使用して、値Ｋ，Ｍ，Ｎ，$\underline{X}_r$の摘要を計算する手段と、C_rを$\underline{X}_r$の所定ビットに挿入する手段との両方に入力される。図１および図２を参照すると、暗号ハッシュ関数を使用して、値の摘要を計算する手段への入力は、Ｋ（ユーザ鍵）、$\underline{X}_r$（修正済み画像ブロック）、Ｍ（元の入力の幅）およびＮ（元の入力ブロックの高さ）である。

【００２７】図１および図２を参照すると、暗号ハッシュ関数を使用して、値Ｋ，Ｍ，Ｎ，$\underline{X}_r$の摘要を計算するステップが示されている。暗号ハッシュ関数は、様々なハッシュ関数から選択される。好ましい実施形態では、周知のＭＤ５関数またはその変形が使用される。ＭＤ５関数は、例えば、R.L.Rivest氏の論文「The MD5 Message Digest Algorithm」（Internet RFC 1321，１９９２年４月）に記述されている。本開示の残りの部分では、ＭＤ５をハッシュ関数として使用するが、他の代替実施形態では他の暗号関数も使用できる。

【００２８】本発明に記載する実施形態では、Ｋは秘密暗号化鍵であり、$\underline{X}_r$は修正した元の入力画像ブロックであり、Ｍは元の入力画像の幅であり、Ｎは元の入力画像の高さである。暗号ハッシュ関数Ｈ（Ｓ）＝（d_1，d_2，…，d_p）を考えてみる。該式で、Ｓは任意の長さのデータ列を表し、ｄｉはハッシュ関数のバイナリ出力ビットであり、ｐはこの出力ビット列のサイズである。入力ビット列Ｓおよびそれに対応する出力（d_1，…，d_p）が与えられたものとして、同じ出力（d_1，…，d_p）にハッシュされる任意の長さの別の入力ビット列を見つけることは、計算上実行不可能である。このＭＤ５ハッシュアルゴリズムを使用して、任意のデータ列が、長さ１２８、すなわちｐ＝１２８のビットアレイ中にハッシュされる。別の暗号関数が使用される場合、長さｐは異なることがある。好ましい実施形態では、不等式ｐ≧ＩＪが満たされる。

【００２９】Ｋをビット列からなるユーザ鍵とする。好ましい実施形態では、各ブロックのデータX_rについて、それに対応するブロック$\underline{X}_r$を形成する。但し、$\underline{X}_r$中の各要素は、最下位ビットがゼロに設定されることを除いて、X_r中の対応する要素に等しい。各ブロックごとに、ハッシュＨ（Ｋ，Ｍ，Ｎ，$\underline{X}_r$）＝（d^r_1，d^r_2，…，d^r_p）を計算する。

【００３０】次いで、ハッシュ出力中の最初のＩＪビットを選択し、サイズＩ×Ｊの長方形アレイ$d_{m,n}$を形成する。

【００３１】ハッシュ出力ｄ（d^r_1，d^r_2，…，d^r_p）および透かし処理されたビットマップB_rのブロックが、ハッシュ出力を透かしと組み合わせる手段に入力される。透かしの抽出と挿入との両方の工程は、このハッシュ出力を透かしB_rと組み合わせるステップを含む。このハッシュ出力１１４を透かし１１８と組み合わせるステップは、ビットごとの論理演算を使用して実行される。これによって、透かし挿入と抽出との両方の工程ための容易な処理が可能になる。好ましい実施形態では、図１および図２に示すように、ビットごとの論理演算は排他的論理和関数である。

【００３２】図１を参照すると、ハッシュ出力アレイがB_rと組み合わされ、ピクセル排他的論理和演算による１ピクセルを使用して、新しいバイナリブロックC_Tが形成される。すなわち、$c_{m,n}=b_{m,n}$ ＸＯＲ d_iを形成する。該式において、ＸＯＲは排他的論理和演算を示す、$c_{m,n}$はC_r中の要素であり、$b_{m,n}$はB_r中の要素であり、d_iはハッシュ出力ｄの要素である。

【００３３】好ましい実施形態では、透かし処理された画像生成前の最後のステップは、修正済み画像$\underline{X}_r$の中に値C_rを挿入することである。修正済み画像ブロック$\underline{X}_r$では、この画像ブロックの少なくとも１ビットが所定値に設定される。通常、C_rは修正されたビットのみに挿入される。修正された各ビットが挿入ビットC_rに対応することが好ましいが、代替の実施形態では、ビットC_rはこの画像ブロックの各修正されたビットに対応せず、したがって、C_rの値はどの修正されたビットの中にも挿入されない。この好ましい実施形態では、この画像ブロックのＬＳＢはゼロに設定されるように修正され、C_rはX_rのＬＳＢの中に挿入され、ある値のC_rが各修正されたビットの中に挿入される。

【００３４】好ましい実施形態では、$c_{m,n}$をブロック$\underline{X}_r$の最下位ビットに置いて、出力ブロックY_rを形成する。この手順は、各ブロックのデータに対して繰り返され、全ての出力ブロックY_rは、透かし処理された画像$Y_{m,n}$を形成するように一緒にアセンブルされる。組み合わせた出力ブロックC_rおよび修正済み画像$\underline{X}_r$は、C_rをX_rの所定ビットに挿入する手段への入力である。C_rを$\underline{X}_r$の所定ビットに挿入する手段の出力は、出力画像ブロックY_rである。出力画像ブロックY_rは、透かし処理された画像ブロックである。

【００３５】図４を参照すると、図１および図２に示す透かし挿入装置および透かし挿入方法とあいまって使用される、透かし抽出装置２００のブロック図が示されている。透かし抽出工程は、画像ブロックY_rから透かしB_rを抽出して、この透かしを引き出す。図４を参照すると、透かし抽出装置２００は、少なくとも１つの所定ビットを所定値に修正する修正手段２１０と、透かし処理された画像ブロックY_rから少なくとも１つの所定ビットを抽出する抽出手段２１８と、修正手段２１０に電気的に結合された、暗号ハッシュ関数を使用して値の摘要を計算する計算手段２１２と、抽出手段２１８に電気的に結合された、ハッシュ出力値２１４を抽出された画像ブロックE_rと組み合わせる組み合わせ手段２１６とを含む。

【００３６】図４および図５に示すフローチャートを参照すると、デジタル画像Y_rから透かしを抽出する方法が示されていて、各Ｉ×Ｊのブロックのために、透かし処理された画像Y_rの少なくとも１つの所定ビットを所定値に修正するステップであって、修正した透かし処理された画像Y_rが$\underline{Y}_r$であるステップ（２５２）と、透かし処理された画像から少なくとも１つの所定ビットを抽出するステップ（２５４）と、暗号ハッシュ関数を使用して値の摘要を計算するステップ（２５６）と、このハッシュ出力を画像ブロックE_rと組み合わせるステップ（２５８）とを含む。

【００３７】図４を参照すると、暗号ハッシュ関数を使用して値Ｋ，Ｍ，Ｎ，$\underline{Y}_r$の摘要を計算するためのブロックへの入力は、Ｋ（ユーザ鍵）、Ｍ（元の画像の画像幅）、Ｎ（元の画像の画像高さ）および$\underline{Y}_r$（画像ブロックの１つの所定ビットを所定値に設定するように修正した透かし処理済み画像ブロック）である。したがって、透かし処理された画像ブロックの１つの所定ビットを所定値に修正するステップ（ステップ２５２）が、暗号ハッシュ関数を使用して、値Ｋ，Ｍ，Ｎ，$\underline{Y}_r$の摘要を計算するステップ（ステップ２５６）の前に実行されなければならない。

【００３８】抽出した透かしを得た後、この抽出した透かしは、（コンピュータ画像比較プログラム等を使用して、視覚的に）適当な透かしと比較することができる。例えば、この適当な透かしは、透かしを比較するために、より早い時期に受信者に送信された画像であってもよい。２つの透かし間に偏差がある場合、偏差の位置が透かし処理された画像内の変更された領域を示す。

【００３９】図６～図１１に、図１、図２、図４および図５に基づく透かし挿入装置および透かし挿入方法と透かし抽出装置および透かし抽出方法を使用して、生成した画像によって現された特性をより明確に示す。例えば、図６および図７によれば、本発明が記載する透かし方法が、不可視の透かし処理を実施することを明瞭にしている。図６を参照すると、透かし挿入前の元の画像を示す。図７に、図１および図２に記述した透かし挿入装置および透かし挿入方法を使用して透かし処理された透かし処理済み画像を示す。図６と図７を比較すると、この２つの画像間に視覚的に観測可能な差がないので、生成した透かしは不可視の透かしである。

【００４０】図８および図９によって明確に示される別の特性は、正しいユーザ鍵が適切な透かしの抽出のために必要なことである。正しいユーザ鍵Ｋを使用し、透かし抽出手順を図７に適用する場合、適切な透かしの存在を示す出力画像図８が得られる。これと対照的に、例えば、画像がマークされないか、不正な鍵が使用されるか、元の画像が切り取られる場合に生じる可能性があるランダムノイズに似た出力画像を図９に示す。画像がマークされない場合、すなわち、画像が透かしを含まない場合、透かし抽出手順は、図９に示すようにランダムノイズに似た出力を返す。同様に、不正な鍵を適用する場合（例えば、鍵を知らない場合）、透かし抽出手順はランダムノイズに似た出力を返す。別の例として、透かし処理された画像が切り取られて、この切り取られた画像上に透かし抽出手順を適用する場合、その出力はランダム雑音に似るはずである。

【００４１】図１０に、ガラスを含むことによって修正された図７の透かし処理された画像を示す。透かし処理された画像に修正（ガラスの添加）を加えた特定の領域を示す、図１０から抽出された透かしを図１１に示す。透かし処理された画像の中のあるピクセルを変更すると、この変更の特定の位置が透かし抽出手順の出力に反映される。図１０に、ガラスが図７上に貼られた画像を示す。また、図１１に、変更が加えられた特定の領域を示す図１０から抽出された透かしを示す。

【００４２】生じる疑問は、透かしがこの画像の最下位ビットに置かれる場合、この透かしは安全であるかということである。この透かしは、認証目的のため、すなわち、この画像に対するどんな変更も検出するように設計されていることを想起されたい。誰かが、この画像のいくつかのビット平面を変更することによって透かしを除去しようとする場合、透かし抽出手順がこの変更を検出することになる。

【００４３】非常に重要な問題は、誰かがこの方式の中に透かしを偽造することが可能であるかどうかというこ

とである。画像ブロックB_rを考えてみる。誰かが、画像ブロックが$\underline{B}_r$になるように、この画像ブロック中のピクセルのいくつかまたは全てを変更したいと仮定する。２つの画像ブロック中のピクセル値が、H（K，M，N，B_r）＝H（K，M，N，$\underline{B}_r$）を満たす必要がある。

【００４４】すなわち、両方の画像ブロックから生成された摘要は同一でなければならない。これは、ＭＤ５アルゴリズム等の暗号ハッシュ関数の特性のために、計算的に実行不可能であると見なされる。

【００４５】図１、図２、図３、図４および図５に示した第１の実施形態では、透かし挿入および透かし抽出を秘密鍵システムに関して説明した。図１２、図１３、図１４および図１５に示した第２の実施形態は、透かし挿入および透かし抽出を公開鍵システムに対して提供する。

【００４６】図１２に、公開鍵システムに関する、元の入力デジタル画像への透かし挿入を実施するための透かし挿入装置のブロック図を示す。図１２に示すブロック図は、図１に示すシステムの修正版であり、公開鍵暗号化を含むように修正が加えられている。同様に、図１４に示すブロック図は、図１４に示す抽出装置が公開鍵解読を含むように修正されていることを除いて、図４に示すシステムを修正したものである。

【００４７】公開鍵暗号化を含むために加えられた修正を除いて（例えば、ハッシュ関数および電気接続への入力が修正された）、一般に図１、図２および図３に対して行われた説明を、図１２および図１３に対しても行うことができる。同様に、図４および図５に対して行われた説明を、図１４および図１５に対して適用する。例えば、画像ブロックX_rが図３に示す代替に基づいて修正される可能性があるという、図１に対して行われた説明は、図１２に対しても当てはまる（実施ブロック９１０は、図１に示す代替に基づいて修正される）。

【００４８】図１２に、公開鍵システムを実施する第２の実施形態に基づく透かし挿入装置のブロック図を示す。また、図１３に、図１２に示す透かし挿入装置に対応するステップのフローチャートを示す。第１の実施形態に規定された画像と同様に、公開鍵システムに関して、Ｍ×Ｎピクセルのサイズを有するグレースケール画像$X_{m,n}$を想定する。透かし処理された画像$Y_{m,n}$を得るために$x_{m,n}$にバイナリの不可視の透かし画像$b_{m,n}$を挿入したい。第１の実施形態と同様に、透かし挿入および透かし抽出は、いくつかのブロックの画像データ上に実行される。便宜上、画像ブロックのサイズを、８×８と選択する。

【００４９】図１２を参照すると、公開鍵システム用の透かし挿入装置９００は、画像ブロックX_rの少なくとも１つの所定ビットを修正する修正手段９１０と、修正手段９１０に電気的に結合された、ハッシュ出力P_rを出力し（９１４）、暗号ハッシュ関数を使用して値の摘要を計算する計算手段９１２と、計算手段９１２に電気的に結合された、ハッシュ出力９１４を透かし９１８と組み合わせる組み合わせ手段９１６と、組み合わせ手段９１６に電気的に結合された公開鍵暗号化手段９２２と、修正手段９１０に電気的に結合された、画像$\underline{X}_r$のブロックの１つの所定ビットに暗号化した出力および透かし（W_r）を挿入する挿入手段９２６とを含む。

【００５０】図１３に、図１２に示す挿入装置に対応するステップのフローチャートを示す。図１３のフローチャートを参照すると、公開鍵システムに関して、デジタルの元の入力画像に透かしを挿入する方法は、Ｉ×Ｊのブロックに元の画像X_rを区分するステップ（９５０）と、各Ｉ×Ｊブロックについて、画像ブロックの少なくとも１つの所定ビットを修正するステップであって、修正済み画像が$\underline{X}_r$であるステップ（９５２）と、暗号ハッシュ関数を使用して値の摘要を計算するステップ（９５４）と、前のステップで計算したハッシュ出力を透かしB_rと組み合わせるステップであって、ハッシュ出力を透かしB_rと組み合わせるステップの出力が合成画像C_rであるステップ（９５６）と、合成画像C_rを暗号化するステップであって、暗号化した画像がW_rであるステップ（９５８）と、修正済み画像ブロック$\underline{X}_r$に値W_rを組み入れるステップ（９６０）とを含む。

【００５１】秘密鍵システム用の透かし挿入に関して記述した方法と同様に、X_rは画像$x_{m,n}$内のｒ番目のデータブロックを示す。次に、１つの所定ビット（最下位ビット）が所定値ゼロに設定されることを除いて、$\underline{X}_r$の中の各要素が$\underline{X}_r$の中の対応する要素と等しい、対応するブロックX_rが形成される。H（・）は、ＭＤ５アルゴリズム等の暗号ハッシュ関数であるとする。このハッシュ関数は、次のように計算される。H（M，N，$\underline{X}_r$）＝（p^r_1，p^r_2，…，p^r_s）

【００５２】該式において、p^r_iはハッシュ関数からの出力ビットを示し、ｓは使用される特定のハッシュ関数に依存する出力ビットのサイズである。例えば、ＭＤ５に対して、ｓ＝１２８である。

【００５３】ビットストリームP_rから第１のＩＪビットを表すと、下式となる。

【００５４】

【数１】

$$P_r \triangleq (p^r_1, p^r_2, \cdots, p^r_{IJ})$$

【００５５】P_rはｂｍ，ｎのビットごとの論理関数であり、通常は排他的論理和関数を使用して、$b_{m,n}$中の対応するブロックB_rと組み合わされる。すなわち、C_r＝P_rＸＯＲ　B_rを計算する。但し、ＸＯＲは２つのブロック間の要素ごとの排他的論理和演算を示す。最後に、公開鍵暗号システムでC_rを暗号化して、W_r＝$E_{K'}$（C_r）を生じる。該式において、E（・）はこの公開鍵システムの暗号化関数であり、K′は個人鍵であ

る。次いで、バイナリブロックのデータW_rは最下位ビットのデータブロック$\underline{X}_r$中に埋め込まれ、透かし処理された画像の中にブロックY_rを形成する。

【００５６】図１４に、図１２および図１３に示す透かし挿入装置および透かし方法と共に使用される透かし抽出装置のブロック図を示す。図１５に、図１４に示す透かし検出装置に使用される、透かし抽出方法のフローチャートを示す。図１４に示す透かし検出装置１０００は、透かし処理された画像Z_rのブロックの少なくとも１つの所定ビットを所定値に修正して、修正済み画像ブロック$\underline{Z}_r$を生成する修正手段１０１０と、画像Z_rから１つの所定ビットを抽出する抽出手段１０１８と、修正手段１０１０が電気的に結合された、暗号ハッシュ関数を使用して値の摘要を計算する計算手段１０１２と、抽出手段１０１８に電気的に結合され、出力が解読された画像ブロックU_rである公開鍵解読手段１０２０と、ハッシュ出力値を解読された画像ブロックU_rと組み合わせる手段であって、ハッシュ出力を修正した画像ブロック$\underline{Z}_r$と組み合わせる該手段が、公開鍵解読手段１０２０と計算手段１０１２とに電気的に結合されている組み合わせ手段１０１６とを含む。

【００５７】抽出手順では、画像ブロックZ_rが、２つの異なる画像を生成するために使用される。好ましい実施形態では、最下位ビットがゼロアウト（zero our）されたことを除いて、第１画像G_rが最下位ビットを含み、他の画像$\underline{Z}_r$がピクセル値を含む。次いで、Ｍ、Ｎおよび$\underline{Z}_r$のハッシュを計算し、出力の最初のＩＪビットをQ_rで示す。公開鍵解読アルゴリズムを使用して、透かし挿入手順に使用した個人鍵Ｋ′に対応する公開鍵ＫでG_rを解読する。すなわち、$U_r=D(G_r)$を計算する。最後に、要素ごとの排他的論理和手順を使用して、出力ブロック$O_r=Q_r$ ＸＯＲ U_rを計算する。

【００５８】公開鍵を用いた透かし挿入および透かし抽出の実施では、ハッシュ関数としてＭＤ５を、暗号化および解読のためにＲＳＡ公開鍵暗号化アルゴリズムを使用した。透かし処理された画像ブロックと画像サイズとの両方が、透かしの挿入以後、変更されなかった場合、すなわち、$Z_r=Y_r$の場合、$\underline{Z}_r=\underline{X}_r$および$G_r=W_r$である。これは、$P_r=Q_r$および$U_r=C_r$であることを意味する。したがって、出力バイナリ画像O_rはブロックB_rと同一である。そうでない場合は、これに該当せず、ハッシュ関数の性質のため、出力ブロックO_rはランダムノイズとほとんど変わらないであろう。結果として、このアルゴリズムは、ピクセル値やブロックレベルに対してのあらゆる変更を検出することができる。

【００５９】図１４に、図１２および図１３に示す透かし挿入装置と透かし挿入方法と組み合わされて使用される透かし抽出装置のブロック図を示す。図１５を参照すると、公開鍵暗号化システムに関して、デジタル画像Y_rから透かしを抽出する方法は、各Ｉ×Ｊのブロックごとに、透かし処理された画像Z_rの少なくとも１つの所定ビットを所定値に修正するステップであって、修正した透かし処理済み画像Z_rが$\underline{Z}_r$であるステップ（１０５０）と、透かし処理された画像$\underline{Z}_r$から、少なくとも１つの所定ビットを抽出するステップであって、この抽出した画像ブロックがG_rであるステップ（１０５４）と、暗号ハッシュ関数を使用して値の摘要を計算するステップ（１０５２）と、公開鍵解読関数$D_k(\cdot)$を使用してG_rを解読するステップであって、この解読された画像ブロックがU_rであるステップ（１０５６）と、ハッシュ出力をこの解読された画像ブロックU_rと組み合わせるステップ（１０５８）とを含むことを示す。

【００６０】図１６に、図１および図２に示す秘密鍵検証方法の特性を要約した実験結果の要約を示す。同様に、図１７に、図１２および図１３に示す公開鍵検証方法の特性を要約した実験結果の要約を示す。図１６および図１７を参照すると、所有権の検証を実施する一方式は、所望の透かしのみを適当なユーザ鍵で透かし処理された画像から抽出することができるように、ユーザ鍵を透かしと関連付けることである。ユーザが不正な鍵を使用したか、または透かし処理されていない画像で透かし抽出手順を実行した場合、ユーザはランダムノイズに似た画像を得る。

【００６１】図１、図２、図３、図４、図５、図１２、図１３、図１４および図１５に示すブロック図およびフローチャートは、ハードウエアまたはソフトウエアのいずれか、あるいは両方の組合せで実施される。例えば、図１のブロック図を参照すると、ハッシュ関数の計算（値の摘要の計算）はソフトウエアで実施することができるが、排他的論理和関数（１１６）および画像ブロックの所定ビットの修正は、ハードウエアで実行することができる。あるいは、別の実施形態では、図１に示すブロック図の実施は、全部ソフトウエアで実施することができるはずであり、ソフトウエアはコンピュータが読取り可能な媒体に記憶され、コンピュータシステム上で動作するように適合される。

【００６２】図１８に、本発明に基づく透かし方法のステップを実施するソフトウエアプログラムを実行するように適合されたコンピュータシステムの高レベルのブロック図を示す。中央演算処理装置（ＣＰＵ）１３１１はバス１３１２に接続され、このバス１３１２はランダムアクセスメモリ（ＲＡＭ）１３１３、読取り専用メモリ（ＲＯＭ）１３１４、入出力（Ｉ／Ｏ）アダプタ１３１５、通信アダプタ１３１６、ユーザインターフェイスアダプタ１３１７およびディスプレイアダプタ１３１８に接続される。ＲＡＭ１３１３とＲＯＭ１３１４は、通常、ユーザおよびシステムのデータとプログラムを記憶する。通常は、本発明を実施するソフトウエアプログラムは記憶媒体上に常駐し、ＣＰＵ上で実行される。

【００６３】上記説明は例示的なものであり、制限する

ものではないことを理解されたい。例えば、本発明は、同じサイズの透かし処理された画像$Y_{m,n}$を形成するために、Ｍ×Ｎ個のピクセルの画像$X_{m,n}$中にデジタル識別子を埋め込むための透かし処理技術を提供する。代替の実施形態では、透かし処理された画像は、画像$X_{m,n}$とは異なるサイズである。したがって、本発明の範囲は、添付の特許請求の範囲と前記特許請求の範囲が受ける権利のある全範囲の均等物と共に参照して決定されるべきである。

【００６４】以下に本発明の実施の形態を要約する。

１．デジタル画像中に透かしを挿入する透かし挿入装置において、画像ブロックX_r中の少なくとも１つの所定ビットを所定値に修正して、修正済み画像ブロック$\underline{X}_r$を生成する第１の修正手段と、前記第１の修正手段に電気的に結合され、暗号ハッシュ関数を使用して値の摘要を計算して、ハッシュ出力を出力する第１の計算手段と、前記第１の計算手段に電気的に結合され、前記ハッシュ出力を透かしと組み合わせて、合成画像ブロックを出力する第１の組み合わせ手段と、前記第１の修正手段に電気的に結合され、前記修正済み画像ブロック$\underline{X}_r$に第１画像ブロックを挿入する挿入手段と、を備えた透かし挿入装置。

【００６５】２．前記第１画像ブロックが前記合成画像ブロックC_rである上記１記載の透かし挿入装置。

【００６６】３．前記第１画像ブロックが暗号化された画像ブロックW_rである上記１記載の透かし挿入装置。

【００６７】４．前記第１の組み合わせ手段が前記挿入手段に電気的に結合される上記２記載の透かし挿入装置。

【００６８】５．前記第１の修正手段が前記画像ブロックX_rのＬＳＢを修正する上記１記載の透かし挿入装置。

【００６９】６．前記第１の組み合わせ手段がＸＯＲ論理ブロックである上記１記載の透かし挿入装置。

【００７０】７．前記第１の修正手段が前記画像ブロックの各カラー平面ごとに独立して少なくとも１つの所定ビットを修正する上記１記載の透かし挿入装置。

【００７１】８．前記第１の組み合わせ手段と前記挿入手段との両方に電気的に結合された暗号化手段をさらに備えた上記３記載の透かし挿入装置。

【００７２】９．デジタル画像から透かしを抽出する透かし抽出装置において、透かし処理された画像の少なくとも１つの所定ビットを所定値に修正する第２の修正手段と、透かし処理された画像ブロックから少なくとも１つの所定ビットを抽出する抽出手段と、前記第２の修正手段に電気的に結合され、暗号ハッシュ関数を使用して値の摘要を計算して、ハッシュ出力を出力する第２の計算手段と、前記第２の計算手段に電気的に結合された第２の組み合わせ手段と、を備えた透かし抽出装置。

【００７３】１０．前記第２の組み合わせ手段が前記抽出手段に電気的に結合される上記９記載の透かし抽出装置。

【００７４】１１．前記抽出手段および前記第２の組み合わせ手段に電気的に結合された解読手段をさらに備えた上記９記載の透かし抽出装置。

【００７５】１２．前記修正手段が前記画像ブロックの最下位のビットを修正する上記９記載の透かし抽出装置。

【００７６】１３．デジタル画像中に透かしを挿入する透かし挿入方法において、少なくとも１つのＩ×Ｊのブロック中に画像ブロックX_rを区分けする区分けステップと、各Ｉ×Ｊブロックごとに、各Ｉ×Ｊブロックの少なくとも１つの所定ビットを所定値に修正して、修正済み画像ブロックが$\underline{X}_r$を生成する修正ステップと、暗号ハッシュ関数を使用して値の摘要を計算する計算ステップと、前のステップで計算したハッシュ出力を透かしビットマップB_rと組み合わせて、合成画像ブロックC_rを出力する組み合わせステップと、前記修正済み画像ブロック$\underline{X}_r$に第１画像ブロックを挿入する挿入ステップと、有する透かし挿入方法。

【００７７】１４．前記第１画像ブロックが前記合成画像ブロックC_rである上記１３記載の透かし挿入方法。

【００７８】１５．前記第１画像ブロックが暗号化された画像ブロックW_rである上記１３記載の透かし挿入方法。

【００７９】１６．暗号化した画像ブロックW_rを生成する前記合成画像ブロックを暗号化する暗号化ステップをさらに有する上記１３記載の透かし挿入方法。

【００８０】１７．前記画像ブロック$\underline{X}_r$の少なくとも１つの所定ビットが前記所定ビットを放棄することによって修正される上記１３記載の透かし挿入方法。

【００８１】１８．前記画像ブロックX_rの少なくとも１つの所定ビットを修正する前記修正ステップが、複数のビットが所定のパターンのビットを所定値に設定することによって修正する上記１３記載の透かし挿入方法。

【００８２】

【発明の効果】以上に詳述したように、本発明のデジタル画像中に透かしを挿入する透かし挿入装置は、画像ブロックX_r中の少なくとも１つの所定ビットを所定値に修正する手段であって、修正済み画像ブロックが$\underline{X}_r$である修正手段と、暗号ハッシュ関数を使用して値の摘要を計算する手段であって、該手段の出力がハッシュ出力であり、修正手段に電気的に結合された計算手段と、ハッシュ出力を透かしと組み合わせる手段であって、該手段の出力が合成画像ブロックであり、計算手段に電気的に結合された組み合わせ手段と、修正済み画像ブロック$\underline{X}_r$に第１画像ブロックを挿入する手段であって、修正手段に電気的に結合された挿入手段とから構成されていることにより、透かしを抽出する透かし抽出装置を用いて透かしを抽出するとき、ピクセル値が変更された場合

のみならず画像サイズの変更の場合も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る透かし挿入装置を示すブロック図である。

【図２】図１に示す透かし挿入装置に対応する透かし挿入方法を示すフローチャートである。

【図３】図２に示された画像ブロックX_rを修正するステップ１５２の代替を示す説明図である。

【図４】図１、図２および図３に示す透かし挿入装置および透かし挿入方法と共に使用される透かし抽出装置を示すブロック図である。

【図５】図１、図２および図３に示す透かし挿入方法と共に使用される透かし抽出方法を示すフローチャートである。

【図６】透かし挿入前の元の画像を示す図である。

【図７】透かし挿入装置および透かし挿入方法を使用して透かし処理を行った画像を示す図である。

【図８】正しいユーザ鍵Ｋが使用されたとき、透かし抽出手順の適用後の抽出した透かし出力画像を示す図である。

【図９】画像がマークされていない、不正な鍵が適用されている、または元の画像が切り取られているなどの場合に生じることのある、ランダムノイズに似た抽出した透かし出力画像を示す図である。

【図１０】ガラスを付加することによって修正した図７の透かし処理を行った画像を示す図である。

【図１１】ガラスの付加によって透かし処理された画像に対する修正が行われた特定の領域を示す図１０から抽出された透かしを示す図である。

【図１２】公開鍵システムを実施する本発明の第２の実施形態に係る透かし挿入装置を示すブロック図である。

【図１３】図１２に示す透かし挿入装置に対応する透かし挿入方法を示すフローチャートである。

【図１４】図１２および図１３に示す透かし挿入装置および透かし挿入方法と共に使用される透かし抽出装置を示すブロック図である。

【図１５】図１２および図１３に示す挿入装置および透かし挿入方法と共に使用される透かし抽出方法を示すフローチャートである。

【図１６】図１および図２に示す秘密鍵検証方法の特性を要約した実験結果の要約を示す図である。

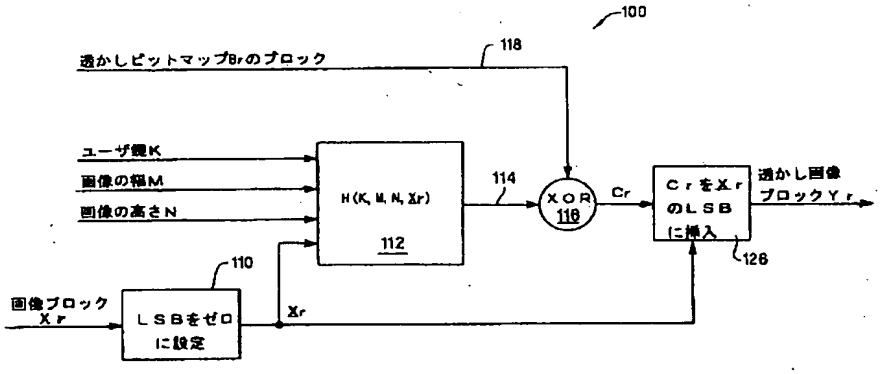
【図１７】図１２および図１３に示す公開鍵検証方法の特性を要約した実験結果の要約を示す図である。

【図１８】本発明の実施形態に係る透かし挿入方法のステップを実施するソフトウエアプログラムを実行するように適合されたコンピュータシステムを示す高レベルのブロック図である。

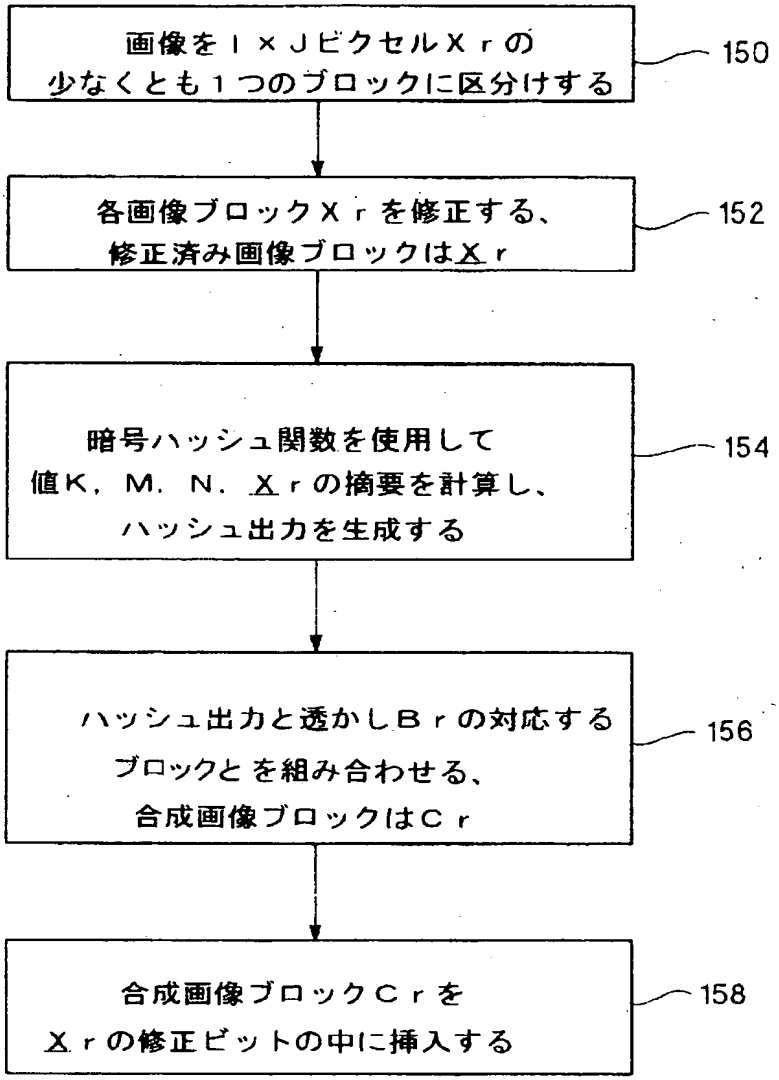
【符号の説明】

１００，９００　透かし挿入装置
１１０，２１０，９１０，１０１０　修正手段
１１２，２１２，９１２，１０１２　計算手段
１１６，２１６，９１６，１０１６　組み合わせ手段
１２６，９２６　挿入手段
２１８，１０１８　抽出手段
２００，１０００　透かし抽出装置
９２２　公開鍵暗号化手段
１０２０　公開鍵解読手段
１３１１　ＣＰＵ
１３１３　ＲＡＭ
１３１４　ＲＯＭ
１３１５　Ｉ／Ｏアダプタ
１３１６　通信アダプタ
１３１７　ユーザインターフェイスアダプタ
１３１８　ディスプレイアダプタ

【図１】



【図２】


画像をＩ×Ｊピクセル Ｘｒの
少なくとも１つのブロックに区分けする
150
各画像ブロックＸｒを修正する、
修正済み画像ブロックはＸｒ
152
暗号ハッシュ関数を使用して
値Ｋ，Ｍ，Ｎ，Ｘｒの摘要を計算し、
ハッシュ出力を生成する
154
ハッシュ出力と透かしＢｒの対応する
ブロックとを組み合わせる、
合成画像ブロックはＣｒ
156
合成画像ブロックＣｒを
Ｘｒの修正ビットの中に挿入する
158

【図６】

【図３】

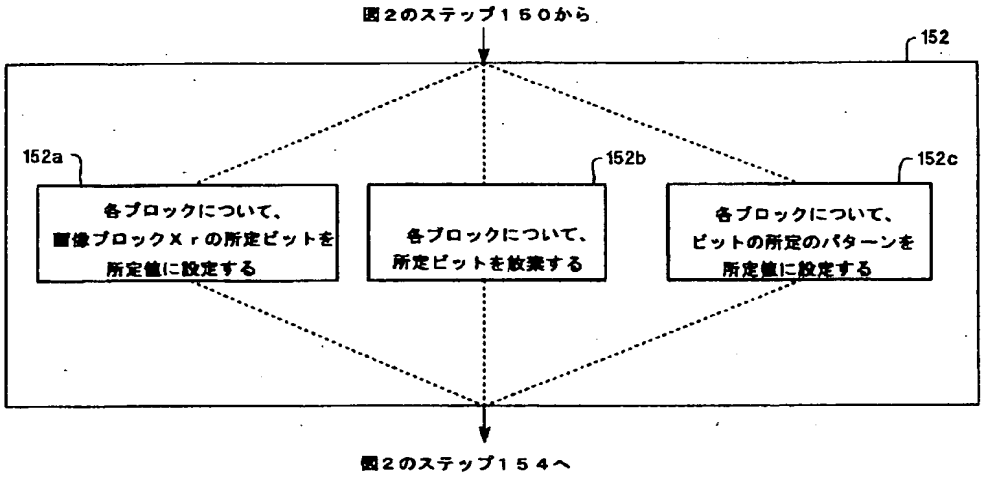
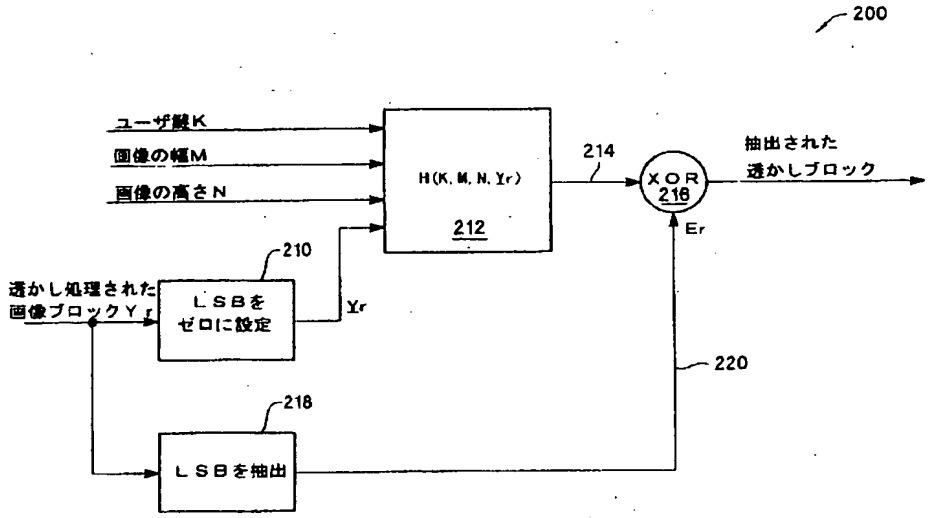
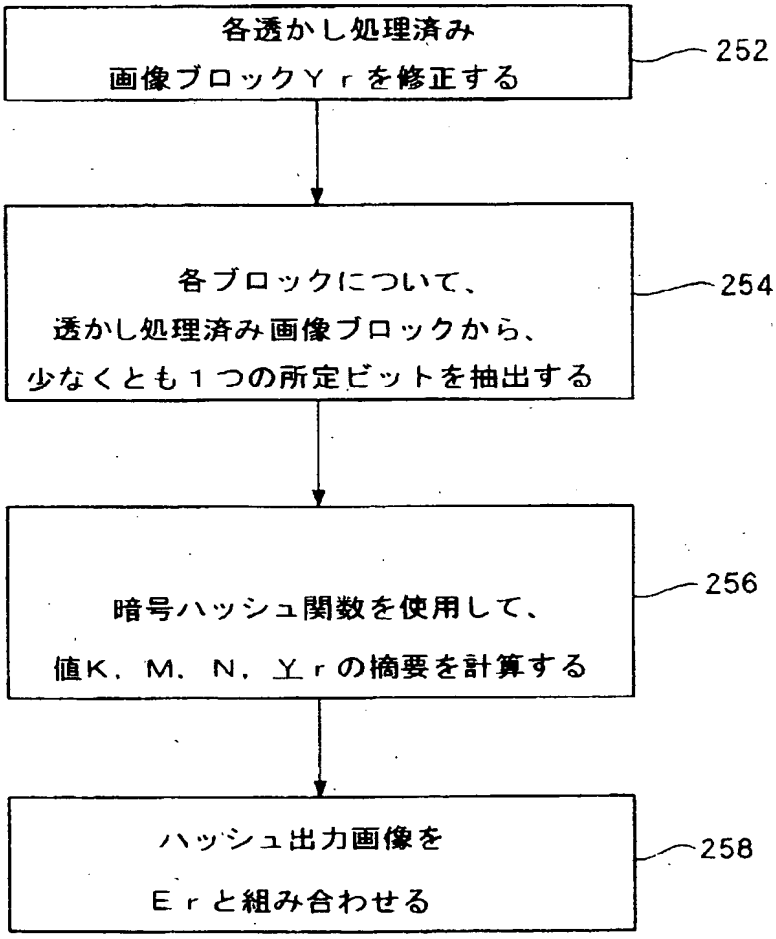


図２のステップ１５０から
152
152a
各ブロックについて、
画像ブロックＸｒの所定ビットを
所定値に設定する
152b
各ブロックについて、
所定ビットを放棄する
152c
各ブロックについて、
ビットの所定のパターンを
所定値に設定する
図２のステップ１５４へ

【図４】

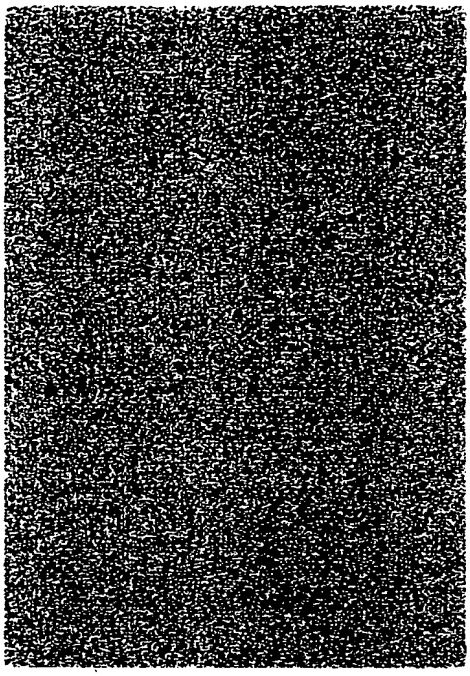

200
ユーザ鍵K
画像の幅M
画像の高さN
H(K, M, N, Yr)
212
214
XOR
216
抽出された
透かしブロック
Er
210
透かし処理された
画像ブロックYr
LSBを
ゼロに設定
Yr
220
218
LSBを抽出

【図５】


各透かし処理済み
画像ブロックＹｒを修正する
252
各ブロックについて、
透かし処理済み画像ブロックから、
少なくとも１つの所定ビットを抽出する
254
暗号ハッシュ関数を使用して、
値Ｋ、Ｍ、Ｎ、Ｙｒの摘要を計算する
256
ハッシュ出力画像を
Ｅｒと組み合わせる
258

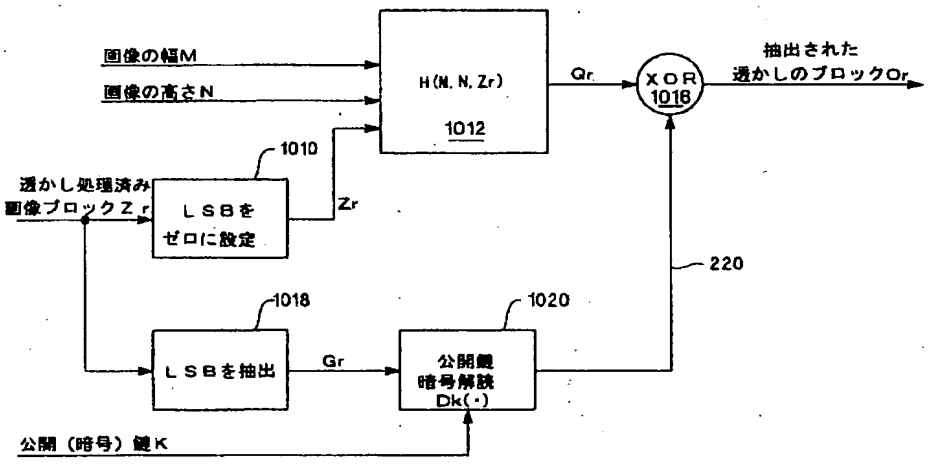
【図７】

【図９】

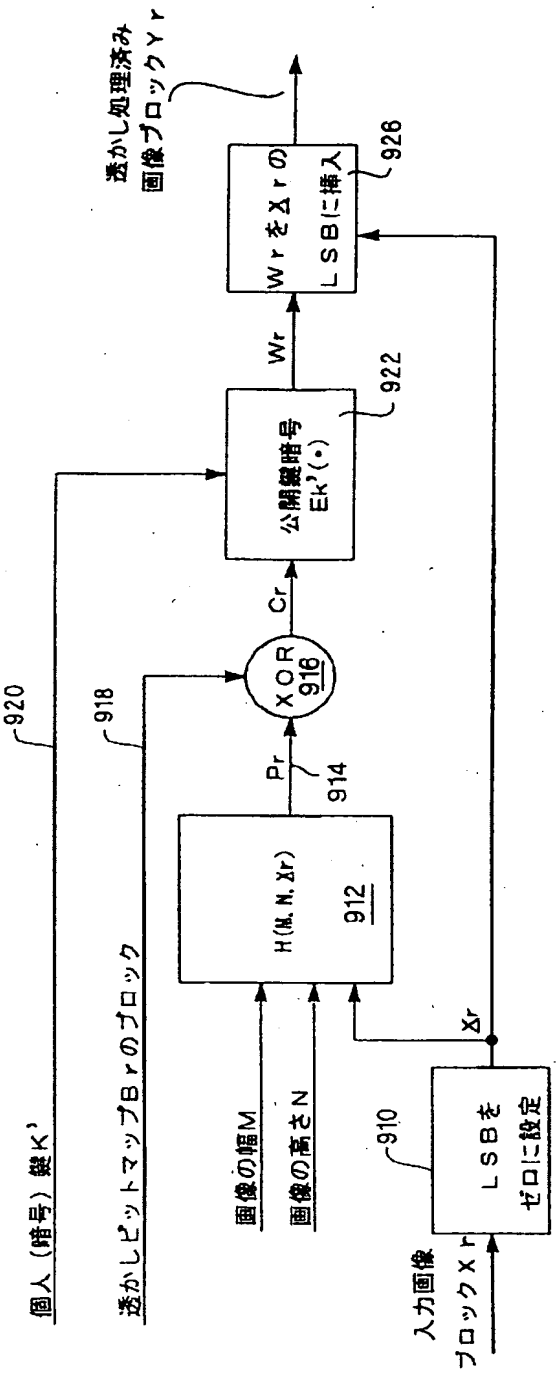


【図１０】

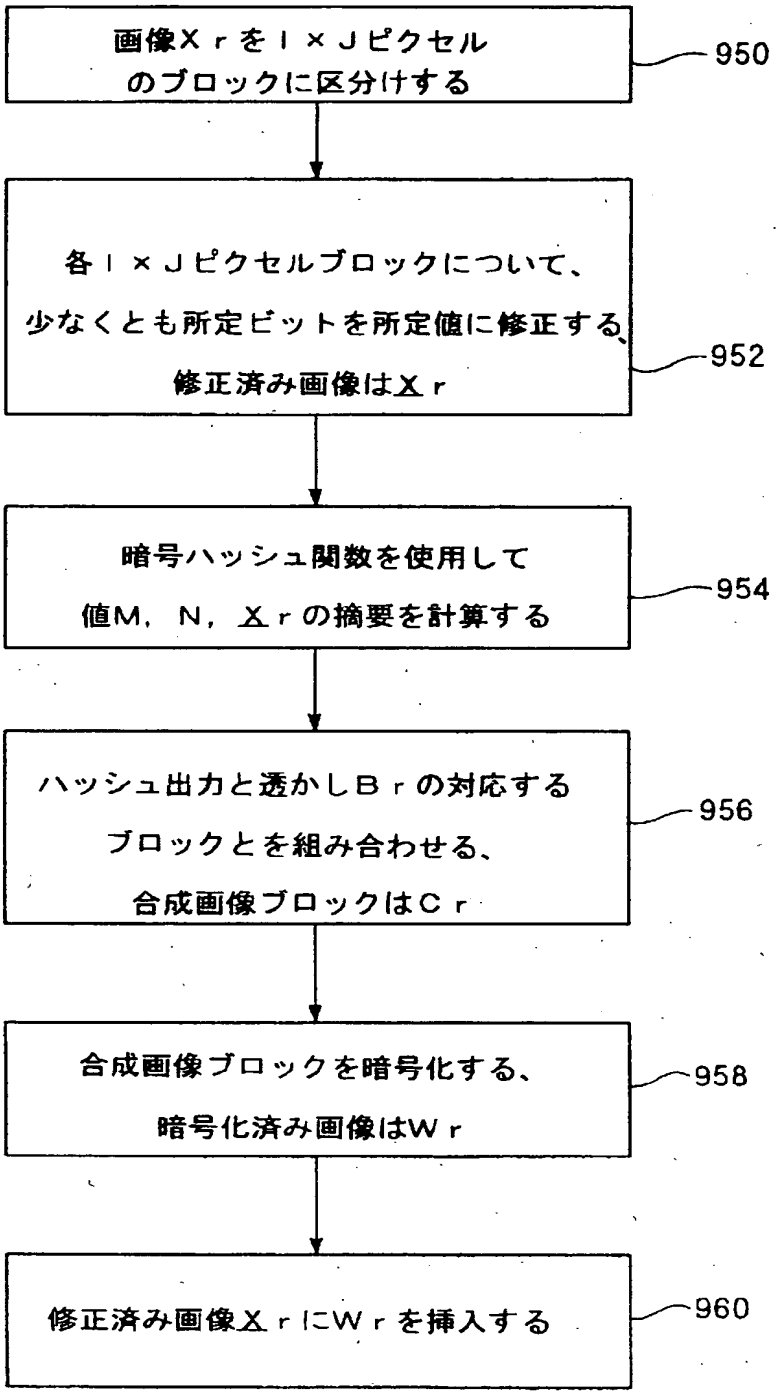
【図１４】


画像の幅M
画像の高さN
H(M, N, Zr)
1012
Qr
XOR
1016
抽出された
透かしのブロックOr
1010
透かし処理済み
画像ブロックZr
LSBを
ゼロに設定
Zr
220
1018
1020
LSBを抽出
Gr
公開鍵
暗号解読
Dk(・)
公開（暗号）鍵K

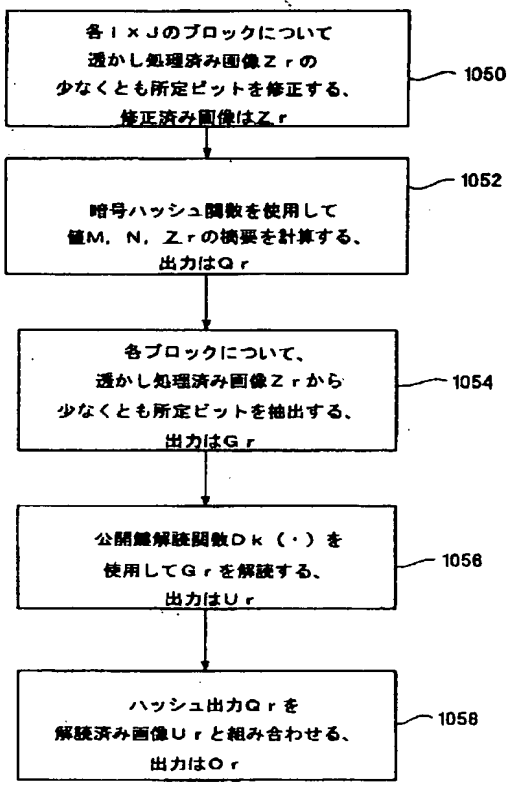
【図１２】


入力画像
ブロックXr
LSBを
ゼロに設定
910
Δr
画像の幅M
画像の高さN
H(M, N, Xr)
912
Pr
914
XOR
916
Cr
公開鍵暗号
Ek'(・)
922
Wr
Wrをxrの
LSBに挿入
926
透かし処理済み
画像ブロックYr
個人（暗号）鍵K'
920
透かしビットマップBrのブロック
918

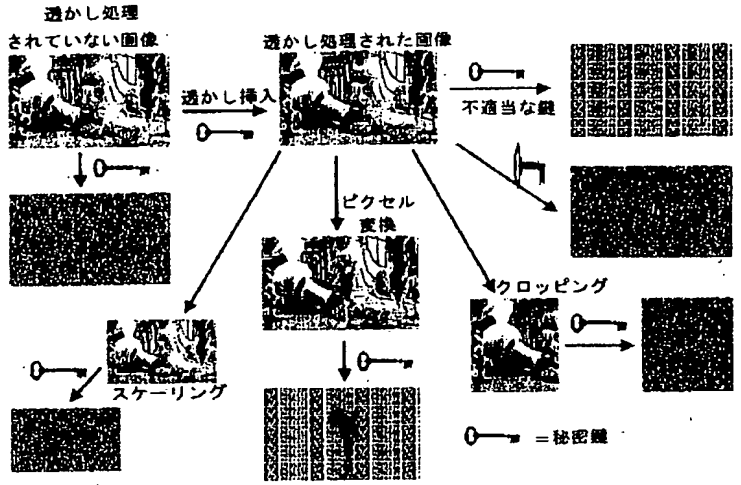
【図１３】


画像Ｘｒを Ｉ×Ｊピクセル のブロックに区分けする
950
各Ｉ×Ｊピクセルブロックについて、少なくとも所定ビットを所定値に修正する、修正済み画像はＸｒ
952
暗号ハッシュ関数を使用して 値Ｍ，Ｎ，Ｘｒの摘要を計算する
954
ハッシュ出力と透かしＢｒの対応する ブロックとを組み合わせる、合成画像ブロックはＣｒ
956
合成画像ブロックを暗号化する、暗号化済み画像はＷｒ
958
修正済み画像ＸｒにＷｒを挿入する
960

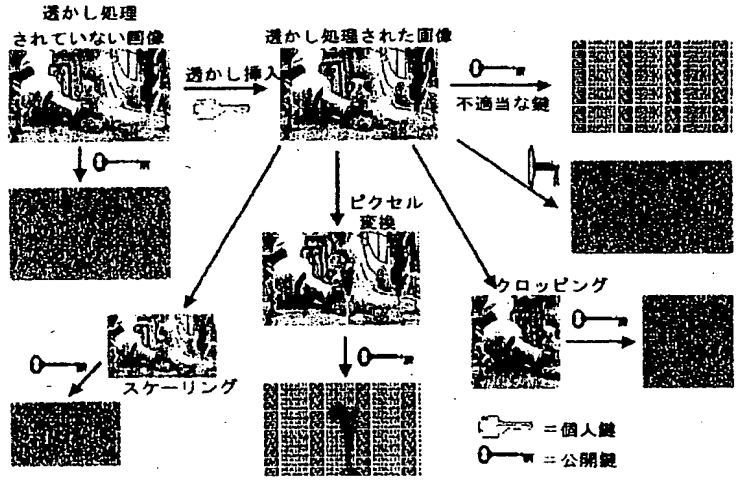
【図１５】


各Ｉ×Ｊのブロックについて 透かし処理済み画像Ｚｒの 少なくとも所定ビットを修正する、修正済み画像はＺｒ
1050
暗号ハッシュ関数を使用して 値Ｍ，Ｎ，Ｚｒの摘要を計算する、出力はＱｒ
1052
各ブロックについて、透かし処理済み画像Ｚｒから 少なくとも所定ビットを抽出する、出力はＧｒ
1054
公開鍵解読関数Ｄｋ（・）を 使用してＧｒを解読する、出力はＵｒ
1056
ハッシュ出力Ｑｒを 解読済み画像Ｕｒと組み合わせる、出力はＯｒ
1058

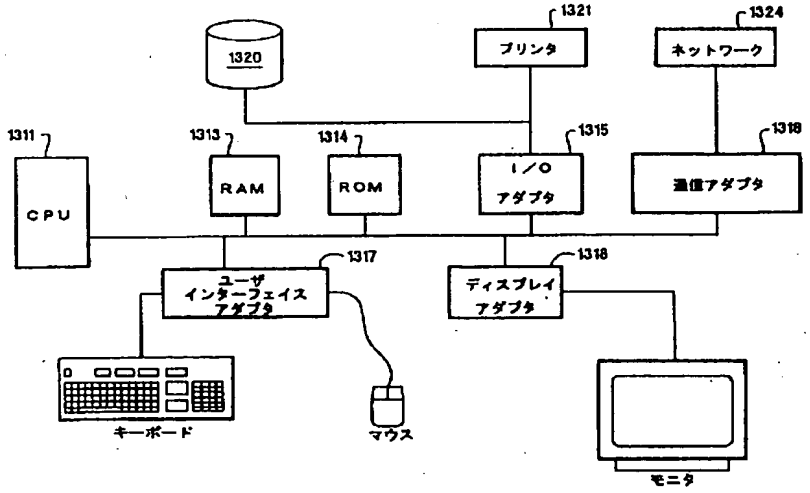
【図１６】


透かし処理
されていない画像
透かし挿入
透かし処理された画像
不適当な鍵
ピクセル
変換
クロッピング
スケーリング
＝秘密鍵

【図１７】


透かし処理
されていない画像
透かし挿入
透かし処理された画像
不適当な鍵
ピクセル
変換
クロッピング
スケーリング
＝個人鍵
＝公開鍵

【図１８】


1320
1321
プリンタ
1324
ネットワーク
1311
CPU
1313
RAM
1314
ROM
1315
I/O
アダプタ
1316
通信アダプタ
1317
ユーザ
インターフェイス
アダプタ
1318
ディスプレイ
アダプタ
キーボード
マウス
モニタ